ESET ENDPOINT SECURITY

POUR ANDROID

Manuel d'installation et guide de l'utilisateur

Cliquez ici pour télécharger la dernière version de ce document.

Sommaire

1. Installation de ESET Endpoint Security..3
1.1 Installation....3
1.2 Désinstallation....4
2. Activation du produit....4
3. Antivirus....4
4. USSD Control....6
5. Antispam....7
6. Anti-vol....8
7. Audit de sécurité....9
8. Administration à distance....10
9. Mise à jour....11
10. Mot de passe....11
11. Dépannage et assistance....12
11.1 Dépannage....12
11.2 Assistance technique....12

ESET **ENDPOINT SECURITY**

Copyright ©2012 par ESET, spol. s r.o.
ESET Endpoint Security a été développé par ESET, spol. s r.o.
Pour plus d'informations, visitez www.eset.com/fr.
Tous droits réservés. Aucune partie de cette documentation ne peut être reproduite, stockée dans un système d'archivage ou transmise sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique, photocopie, enregistrement, numérisation ou autre, sans l'autorisation écrite de l'auteur.
ESET, spol. s r.o. se réserve le droit de modifier les applications décrites sans préavis.

Service client : http://support.athena-gs.fr/demande_de_support.php?editeur=eset

Rév. 17. 12. 2012

1. Installation de ESET Endpoint Security

Pour que vous puissiez installer ESET Endpoint Security pour Android, votre appareil mobile doit disposer de la configuration système suivante :

	Configuration système minimum
Système d'exploitation	Android 2.1 (Eclair) et version ultérieure
CPU	600 MHz
RAM	256 Mo
Espace disponible dans la zone de stockage interne	5 Mo

REMARQUE : certaines fonctionnalités telles que Antispam et Anti-Theft ne sont pas disponibles sur les tablettes/ Android 3.0 ne prenant pas en charge les appels et la messagerie. Vous trouverez plus de détails dans cet article de la Base de connaissances (peut ne pas être disponible dans votre langue).

1.1 Installation

Utilisez l'une des méthodes suivantes pour installer ESET Endpoint Security :

- Téléchargez le fichier d'installation ESET Endpoint Security *(ees.apk)* depuis le site Web d'ESET en numérisant le code QR ci-dessous à l'aide d'une application telle que QR Droid ou Barcode Scanner :

- Téléchargez le fichier *ees.apk* sur votre ordinateur depuis le site Internet d'ESET. Copiez le fichier sur votre appareil par Bluetooth ou USB. Appuyez sur l'icône de lancement de l'écran d'accueil Android, ou sélectionnez **Accueil** > **Menu** et appuyez sur **Paramètres** > **Applications.** Veillez à ce que l'option **Sources inconnues** soit sélectionnée. Recherchez le fichier *ees.apk* à l'aide d'une application du type ASTRO File Manager ou ES File Explorer. Ouvrez le fichier et appuyez sur **Installer**. Une fois l'application installée, appuyez sur **Ouvrir**.

- Si vous souhaitez installer et activer ESET Endpoint Security sur plusieurs appareils, créez un fichier de configuration xml dans ESET Configuration Editor.

  Ouvrez ESET Configuration Editor à partir de ERA Console (**Outils** > ESET Configuration Editor) ou cliquez sur **Démarrer** > **Tous les programmes** > **ESET** > ESET Remote Administrator **Console >** ESET Configuration Editor. Dans l'arborescence de gauche, sélectionnez **Appareils mobiles** > **Endpoint Security pour Android** > **Mettre à jour** > **Paramètres** > **Nom d'utilisateur**. Entrez votre nom d'utilisateur (données de licence reçues de ESET après l'achat du produit) dans le champ **Valeur** sur la droite, puis cliquez sur **Suivant**. Cliquez sur le bouton **Définir un mot de passe** et entrez votre mot de passe. Cliquez sur **OK** pour confirmer. Vous pouvez également définir des paramètres supplémentaires (ex., paramètres d'administration à distance ou antivirus) que vous souhaitez appliquer à tous les appareils mobiles à l'aide de ESET Configuration Editor. Lorsque vous avez terminé les modifications, cliquez sur **Fichier** > **Enregistrer** (ou appuyez sur Ctrl+S) et enregistrez le fichier sous *settings.xml*.

  Copiez le fichier que vous venez d'enregistrer dans le dossier racine de votre carte SD *(/mnt/sdcard)* avec le fichier d'installation de ESET Endpoint Security *ees.apk* (disponible ici). Ouvrez le fichier *ees.apk* dans une application telle que ASTRO File Manager ou ES File Explorer et appuyez sur **Installer**. Une fois l'installation terminée, appuyez sur **Ouvrir**. ESET Endpoint Security s'active automatiquement en utilisant le nom d'utilisateur et le mot de passe enregistrés dans le fichier *settings.xml*.

Avertissement : ESET Endpoint Security doit être installé sur l'espace de stockage interne de l'appareil. Certains téléphones mobiles autorisent les utilisateurs à installer des applications sur la carte SD. Si vous installez ESET Endpoint Security sur votre carte SD, les fonctions Protection en temps réel, Antispam et Anti-vol ne fonctionneront pas.

Une fois ESET Endpoint Security installé, vous devez l'activer en suivant les étapes de la section Activation du produit 4.

1.2 Désinstallation

Pour désinstaller ESET Endpoint Security de votre appareil mobile, utilisez l'option **Assistant de désinstallation** accessible depuis le menu principal de ESET Endpoint Security ou effectuez les opérations ci-dessous :

1. Appuyez sur l'icône de lancement de l'écran d'accueil Android (ou sélectionnez **Accueil** > **Menu**). Appuyez ensuite sur **Paramètres** > **Localisation et sécurité** > **Administrateurs**, désélectionnez **ESET Security** et appuyez sur **Désactiver**. Entrez votre mot de passe ESET Endpoint Security lorsque le système vous le demande. (Si vous n'avez pas défini ESET Endpoint Security en tant qu'administrateur de l'appareil, ignorez cette étape.)
2. Revenez à **Paramètres** et appuyez sur **Applications** > **Gérer applications** > **ESET Security**> **Désinstaller**.

ESET Endpoint Security et le dossier de quarantaine sont supprimés de manière permanente de votre appareil mobile.

2. Activation du produit

Après son installation, ESET Endpoint Security doit être activé. Appuyez sur **Activer maintenant** dans le menu principal de ESET Endpoint Security.

Activer à l'aide d'un nom d'utilisateur et d'un mot de passe - Entrez le nom d'utilisateur et le mot de passe (données de licence fournies parESET lors de l'achat du produit) dans les champs correspondants.

Chaque activation n'est valide que pour une durée déterminée. Une fois l'activation expirée, vous serez invité à renouveler la licence du programme (le programme vous en avertira à l'avance).

REMARQUE : pendant l'activation, l'appareil doit être connecté à Internet. Des données seront téléchargées.

Par défaut, ESET Endpoint Security est installé dans la langue qui est définie dans les paramètres régionaux de votre téléphone (dans les paramètres de langue et de clavier). Pour changer la langue de de l'interface utilisateur de l'application, sélectionnez **Langue** dans le menu principal de ESET Endpoint Security et sélectionnez la langue de votre choix.

3. Antivirus

Analyser l'appareil

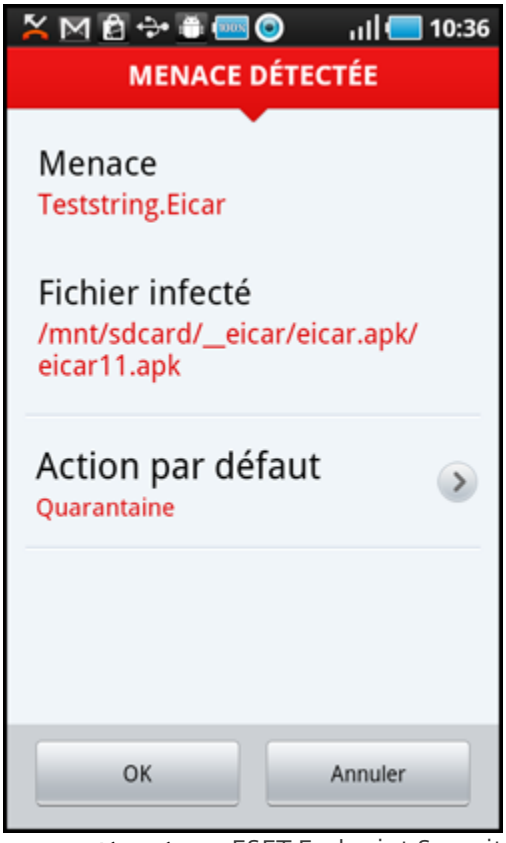
Analyser l'appareil permet de rechercher la présence éventuelle d'infiltrations sur votre appareil mobile.

Certains types de fichiers prédéfinis sont analysés par défaut. Une analyse complète de l'appareil vérifie la mémoire, les processus en cours, les DLL (bibliothèques de liaison dynamiques) qui en dépendent, ainsi que les fichiers faisant partie de la zone de stockage interne et des supports amovibles. Une fois l'analyse terminée, un récapitulatif des résultats apparaît : nombre de fichiers infectés, nombre de fichiers analysés, durée de l'analyse, etc.).

Pour interrompre une analyse en cours, appuyez sur **Annuler**.

Analyser le dossier

Pour analyser certains dossiers de votre appareil, appuyez sur **Analyser le dossier**. Recherchez les dossiers à analyser, cochez les cases correspondantes dans la colonne de droite et appuyez sur **Analyse**.



Menace détectée par ESET Endpoint Security

Journaux d'analyse

La section **Journaux d'analyse** contient des journaux qui fournissent des informations complètes sur les tâches d'analyse réalisées. Les journaux sont créés à chaque analyse déclenchée manuellement (à la demande) ou lorsqu'une infiltration a été détectée par l'analyse en temps réel.

Chaque journal contient les éléments suivants :

- la date et l'heure de l'événement ;
- le nombre de fichiers analysés ;
- le nombre de fichiers infectés ;
- le nom et le chemin d'accès complet des fichiers infectés ;
- la durée de l'analyse ;
- les actions exécutées ou les erreurs rencontrées lors de l'analyse.

Quarantaine

La principale fonction de la quarantaine consiste à stocker les fichiers infectés en toute sécurité. Les fichiers doivent être placés en quarantaine s'ils ne peuvent pas être nettoyés, s'il est risqué ou déconseillé de les supprimer, ou encore s'ils sont détectés à tort par ESET Endpoint Security.

Les fichiers stockés en quarantaine peuvent être affichés dans un journal qui indique le nom et l'emplacement d'origine des fichiers infectés, ainsi que la date et l'heure de leur mise en quarantaine.

Si vous souhaitez restaurer un fichier mis en quarantaine dans son emplacement d'origine, appuyez sur le fichier et sélectionnez **Restaurer**. Cette option n'est pas recommandée.

Pour supprimer de manière permanente un fichier mis en quarantaine de votre appareil, appuyez sur le fichier et sélectionnez **Supprimer**. Pour supprimer tous les fichiers stockés dans la quarantaine, appuyez sur le bouton **MENU**, puis sur **Supprimer tout**.

Paramètres

Les paramètres **À la demande** permettent de modifier les paramètres d'analyse à la demande (déclenchée manuellement).

L'option **Boîte de dialogue Afficher les alertes** affiche des notifications d'alerte chaque fois qu'une nouvelle menace est détectée par l'analyse à la demande.

Si vous souhaitez analyser toutes les applications (fichiers *.apk*) installées sur l'appareil, sélectionnez **Analyser les applications**.

La **protection proactive** est une méthode de détection basée sur un algorithme, qui analyse le code et recherche tout comportement typique de virus. Elle permet notamment d'identifier les logiciels malveillants qui ne sont pas encore identifiés par la version actuelle de la base des signatures de virus. Si la protection proactive est activée, l'analyse est plus longue.

L'option **Profondeur d'analyse des archives** permet d'indiquer le nombre de niveaux d'imbrication des archives (fichiers *.zip*) à analyser. Plus le nombre est élevé, plus l'analyse « descend » dans les différents niveaux d'imbrication.

L'option **Stockage des journaux** permet de définir le nombre maximum de journaux à stocker dans la section **Journaux d'analyse** 5.

Vous pouvez indiquer une **action par défaut** qui sera exécutée automatiquement en cas de détection de fichiers infectés. Les actions suivantes peuvent être définies par défaut :

- **Ignorer** - Aucune action n'est effectuée sur le fichier infecté (cette option n'est pas recommandée).
- **Supprimer** - Le fichier infecté est supprimé.
- **Quarantaine** (option par défaut) - Le fichier infecté est placé en **quarantaine** 5.

Les paramètres **Extensions** répertorient les types de fichiers les plus courants qui sont les plus exposés aux infiltrations sur la plateforme Android. Sélectionnez les types de fichiers à analyser ou désélectionnez les extensions à exclure de l'analyse. Ces paramètres s'appliquent à l'analyse à la demande et à l'analyse en temps réel :

- **Sensible aux extensions** - Si vous sélectionnez cette option, seuls les fichiers portant les extensions spécifiées sont analysés, ce qui permet de réduire le temps nécessaire à l'analyse. Nous vous recommandons de désactiver cette fonctionnalité périodiquement afin de permettre à ESET Endpoint Security de rechercher tous les types d'infiltrations possibles, notamment celles dissimulées derrière de fausses extensions de fichiers.
- **DEX (fichier du code applicatif)** - Format de fichier exécutable contenant le code compilé écrit pour le système d'exploitation Android.
- **SO (bibliothèques)** - Bibliothèques partagées, enregistrées aux emplacements indiqués du système de fichiers et liées par les programmes qui les utilisent.
- **Archives (fichiers compressés)** - Fichiers compressés (fichiers zip).
- **Autres** - Autres types de fichiers connus.

Dans les paramètres **En temps réel**, vous pouvez configurer les paramètres de l'analyse à l'accès. L'analyse à l'accès vérifie en temps réel les fichiers que vous manipulez. Elle vérifie automatiquement le dossier des *éléments téléchargés* sur la carte SD, les fichiers d'installation *.apk*, ainsi que les fichiers de la carte SD après son montage (si l'option **Analyser les cartes SD montées** est activée). L'analyse à l'accès est lancée automatiquement au démarrage du système.

- **Protection en temps réel** - Si cette option est activée (par défaut), l'analyse à l'accès s'exécute en arrière-plan.
- **Boîte de dialogue Afficher les alertes** - Affiche des notifications d'alerte chaque fois qu'une nouvelle menace est détectée par l'analyse à l'accès.
- **Analyser les cartes SD montées** - Analyse les fichiers avant de les ouvrir ou de les enregistrer sur la carte SD.
- **Protection proactive** - Sélectionnez cette option pour appliquer les techniques d'analyse heuristique. L'analyse heuristique identifie de manière proactive les nouveaux logiciels malveillants que la version actuelle de la base des signatures de virus ne détecte pas encore : elle analyse le code et reconnaît le comportement typique des virus. Si la protection proactive est activée, l'analyse est plus longue.
- **Profondeur d'analyse des archives** - Cette option permet d'indiquer le nombre de niveaux d'imbrication des archives (fichiers *.zip*) à analyser. Plus le nombre est élevé, plus l'analyse « descend » dans les différents niveaux d'imbrication.
- **Action par défaut** - Vous pouvez indiquer une action par défaut qui sera exécutée automatiquement en cas de détection de fichiers infectés lors de l'analyse à l'accès. Si vous sélectionnez **Ignorer**, aucune action n'est effectuée sur le fichier infecté (cette option n'est pas recommandée). Si vous sélectionnez **Supprimer**, le fichier infecté est supprimé. Si vous sélectionnez **Quarantaine**, le fichier infecté est placé en **quarantaine** 5.

L'icône de notification d'ESET Endpoint Security est affichée dans l'angle supérieur gauche de l'écran (barre d'état Android). Si vous ne souhaitez pas que cette icône apparaisse, affichez le menu principal de ESET Endpoint Security, appuyez sur le bouton **MENU**, puis sur **Paramètres de notification** et désélectionnez **Afficher l'icône**. Veuillez noter qu'en cas de risque de sécurité (analyse antivirus en temps réel désactivée, correspondance SIM désactivée, etc.), l'icône rouge d'avertissement avec point d'exclamation continue à s'afficher.

4. USSD Control

La dernière version de ESET Endpoint Security (1.2.103 et versions ultérieures) protège votre appareil d'un effacement à distance et d'autres attaques USSD. Les codes USSD (Unstructured Supplementary Service Data) peuvent être exécutés par des messages texte, des codes QR ou des liens URL malveillants.

Si vous recevez une notification indiquant qu'une nouvelle de ESET Endpoint Security est disponible pour téléchargement, ESET vous recommande de l'installer dès que possible.

USSD Control n'est pas accessible à partir du menu principal, mais fonctionne en arrière-plan et ne vous avertit que lorsqu'une commande USSD est exécutée. Pour vérifier en toute sécurité la vulnérabilité de votre appareil au code USSD, suivez les instructions des étapes 4-6 de cet article de la Base de connaissances.

5. Antispam

Le module **Antispam** bloque les SMS/MMS entrants, ainsi que les appels entrants/sortants en fonction des règles que vous déterminez.

Les messages non sollicités concernent habituellement des annonces de prestataires de service de téléphone portable, ou des messages d'inconnus ou d'utilisateurs non spécifiés. L'expression *blocage de message* fait référence au placement automatique d'un message entrant dans la section **Journaux de courrier indésirable** 7. Aucune notification n'est affichée lorsqu'un message entrant est bloqué. Avec cette fonction, vous n'êtes pas dérangé par des informations non sollicitées, mais vous avez toujours la possibilité de consulter la liste des messages bloqués afin de vous assurer qu'aucun message n'a été bloqué par erreur.

Pour ajouter une nouvelle règle antispam, touchez les options **Liste des règles SMS et Appels** > **Ajouter nouveau**. Saisissez le numéro de téléphone que vous souhaitez bloquer ou appuyez sur le bouton **+** pour le sélectionner dans la liste des contacts. Personnalisez la règle en autorisant ou bloquant des messages et des appels, puis appuyez sur **OK**.

Pour modifier ou supprimer une entrée de règle existante, appuyez de manière prolongée sur l'entrée et choisissez l'option souhaitée dans la liste qui apparaît. Si vous souhaitez supprimer toutes les règles antispam, appuyez sur le bouton **MENU**, puis sur **Supprimer tout**.

REMARQUE : le numéro de téléphone doit inclure l'indicatif international, suivi du numéro proprement dit (par exemple +161010010O).

Liste des règles antispam

Paramètres

Bloquer les appels anonymes - Activez cette option si vous souhaitez bloquer les appelants dont le numéro de téléphone a volontairement été masqué par l'intermédiaire de la fonction de refus de présentation de la ligne appelante (CLIR ou Calling Line Identification Restriction).

Bloquer les contacts connus - Utilisez cette option pour bloquer les messages et les appels des contacts figurant dans votre liste de contacts.

Bloquer les contacts inconnus - Cette option bloque les messages et les appels des personnes ne figurant pas dans votre liste de contacts. Vous pouvez utiliser cette option pour bloquer les appels indésirables ou pour empêcher vos enfants de composer des numéros inconnus. (Pour éviter cela, il est recommandé de protéger les paramètres antispam par un **mot de passe** 11.)

Dans la section **Journaux de courrier indésirable**, vous pouvez voir les appels et messages bloqués par le module de blocage du courrier indésirable. Chaque journal contient le nom de l'événement, le numéro de téléphone correspondant, ainsi que la date et l'heure de l'événement. Les SMS bloqués contiennent également le corps du message.

6. Anti-vol

La fonctionnalité **Anti-vol** protège votre téléphone mobile de tout accès non autorisé.

Si vous perdez votre téléphone, ou si quelqu'un le vole et remplace votre carte SIM par une autre carte (non fiable), le téléphone est verrouillé automatiquement par ESET Endpoint Security. Un SMS d'alerte est envoyé aux numéros de téléphone indiqués par l'utilisateur. Ce message indique le numéro de la carte SIM insérée dans l'appareil, le numéro IMSI (numéro d'identité internationale d'abonné mobile), ainsi que le numéro IMEI (numéro d'identité internationale d'équipement mobile) de l'appareil mobile. L'utilisateur non autorisé n'a pas conscience que ce message a été envoyé puisqu'il est supprimé automatiquement des fils des **messages**. Vous pouvez également demander les coordonnées GPS du téléphone qui a été perdu ou effacer à distance toutes les données stockées sur le téléphone.

Cartes SIM de confiance

Cette fonctionnalité n'est pas disponible sur les appareils sans carte SIM (tablettes et téléphones CDMA).

Si la carte SIM qui est insérée dans votre appareil mobile est celle que vous souhaitez enregistrer comme étant fiable, appuyez sur le bouton **Ajouter**. Si vous utilisez plusieurs cartes SIM, vous souhaiterez peut-être les différencier en modifiant l'**alias de la carte SIM** (en indiquant par exemple *Bureau* ou *Maison*).

Pour **modifier** ou **supprimer** une entrée de carte SIM existante, appuyez de manière prolongée sur l'entrée et sélectionnez l'option souhaitée dans la liste qui apparaît. Si vous souhaitez supprimer toutes les entrées de la liste, appuyez sur le bouton **MENU**, puis sur **Supprimer tout**.

Contacts administrateur

Dans la liste **Contacts administrateur**, **ajoutez** les numéros de téléphone qui recevront le SMS d'alerte si une carte SIM non fiable est insérée dans votre appareil. Saisissez un nom dans le champ **Nom du contact** et le numéro de téléphone dans le champ **Numéro de téléphone**, ou appuyez sur le bouton **+** pour sélectionner un contact dans la liste des contacts. Si le contact comporte plusieurs numéros de téléphone, le SMS d'alerte est envoyé à tous ces numéros.

Pour **modifier** ou **supprimer** une entrée existante, appuyez de manière prolongée sur l'entrée et sélectionnez l'option souhaitée dans la liste qui apparaît. Si vous souhaitez supprimer toutes les entrées de la liste, appuyez sur le bouton **MENU**, puis sur **Supprimer tout**.

REMARQUE : le numéro de téléphone doit inclure l'indicatif international, suivi du numéro proprement dit (par exemple +161010O10O).

Paramètres

Si vous ne souhaitez pas utiliser la mise en correspondance SIM, sélectionnez l'option **Ignorer la mise en correspondance SIMg**. Les avertissements *Risque de sécurité* affichés en rouge (concernant la *désactivation de la mise en correspondance SIM* et l'*absence de définition d'une carte SIM fiable*) sont alors désactivés dans le menu principal de ESET Endpoint Security. L'option Ignorer la mise en correspondance SIM est grisée sur les appareils CDMA.

Pour activer la vérification automatique de la carte SIM insérée dans l'appareil (et l'envoi d'un SMS d'alerte), sélectionnez **Activer la correspondance SIM**.

Dans le champ **Texte de l'alerte SMS**, vous pouvez modifier le message qui sera envoyé au(x) numéro(s) prédéfini(s) si une carte SIM non fiable est insérée dans votre appareil. Vous pouvez également entrer une autre adresse de messagerie ou un autre numéro de contact.

Commandes SMS

Les commandes à distance SMS (« wipe », « lock » et « find ») ne fonctionnent que si **Activer les commandes par SMS** est sélectionné.

L'option **Activer la réinitialisation du mot de passe par SMS** vous permet de réinitialiser votre mot de passe de sécurité en envoyant à votre appareil mobile un SMS depuis un appareil que vous avez enregistré dans la liste **Contacts administrateur**. Ce SMS doit avoir la forme suivante :
eset remote reset

Si vous avez perdu votre appareil et souhaitez le verrouiller, envoyez à votre numéro un SMS de verrouillage à distance depuis un appareil mobile. Le SMS doit avoir le format suivant :
eset lock mot_de_passe
Remplacez *mot_de_passe* par le mot de passe que vous avez défini dans la section **Mot de passe** 11. Un utilisateur non autorisé ne pourra pas utiliser votre téléphone, car il devra entrer votre mot de passe.

Si vous souhaitez demander les coordonnées GPS de votre appareil mobile, envoyez un SMS de recherche à distance à votre numéro d'appareil mobile ou au numéro d'un utilisateur non autorisé (selon que la carte SIM a déjà été remplacée ou non) :
eset find mot_de_passe
Vous allez recevoir un SMS indiquant les coordonnées GPS et un lien vers Google Maps qui vous permettra de localiser avec précision votre appareil mobile. Veuillez noter que, pour recevoir les coordonnées GPS, vous devez activer au préalable le module GPS sur votre appareil.

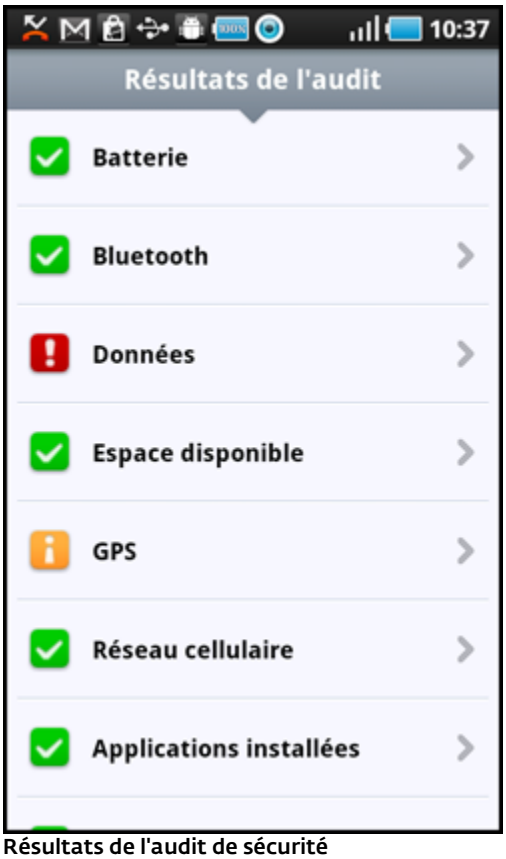
Si vous souhaitez effacer toutes les données stockées sur votre appareil et sur tous les supports amovibles qui y sont insérés, envoyez un SMS de suppression à distance :
eset wipe mot_de_passe
Tous les contacts, SMS, messages électroniques, applications installées, ainsi que votre compte Google et le contenu de la carte SD, sont effacés de manière permanente de votre appareil. Si ESET Endpoint Security n'est pas défini comme Administrateur de l'appareil, seuls les contacts, les messages et le contenu de la carte SD sont effacés.

REMARQUE : Votre mot de passe fait la différence entre les majuscules et les minuscules. Veillez par conséquent à le saisir exactement comme vous l'avez défini dans la section Mot de passe.

7. Audit de sécurité

L'**Audit de sécurité** vérifie différentes données concernant le téléphone : niveau de la batterie, statut Bluetooth, espace disque libre, etc.

Pour exécuter un audit de sécurité manuellement, appuyez sur **Audit**. Un rapport détaillé apparaît.



Résultats de l'audit de sécurité

La coche verte située à côté de chaque élément indique que la valeur est au-dessus de la limite ou que l'élément ne représente pas un risque de sécurité.

L'icône orange indique que la valeur d'un des éléments est au-dessous de la limite ou que l'élément pourrait représenter un risque de sécurité potentiel. Appuyez sur l'élément pour afficher les résultats détaillés.

Le point d'exclamation rouge indique que l'élément est au-dessous de la limite ou qu'il représente un risque de sécurité qui doit être résolu.

Si vous souhaitez résoudre l'état de l'élément en rouge, appuyez sur l'élément et confirmez en appuyant sur **Oui**.

Paramètres

L'audit de sécurité est planifié pour s'exécuter par défaut toutes les 24 heures. Si vous souhaitez désactiver les audits périodiques, désélectionnez l'option **Audit périodique**.

Si **Correction automatique** est activé, ESET Endpoint Security essaie automatiquement de corriger les éléments présentant un risque (par exemple le statut Bluetooth) sans intervention de l'utilisateur. Cette option ne s'applique qu'à l'audit automatique (planifié).

L'option **Stockage des journaux** permet de définir le nombre maximum de journaux à stocker dans la section **Journaux d'audit**.

L'option **Période d'audit** permet de définir la fréquence de l'audit automatique (planifié).

Pour modifier la limite à partir de laquelle l'espace disque disponible et le niveau de batterie sont considérés faibles, utilisez les options **Limite d'espace libre du disque** et **Limite du niveau de batterie**.

Dans l'onglet **Éléments à vérifier**, sélectionnez les éléments à vérifier au cours de l'audit périodique (planifié).

La section **Journaux d'audit** contient des journaux qui fournissent des informations complètes sur les audits périodiques et déclenchés manuellement. Chaque journal contient la date et l'heure de l'événement, ainsi que les résultats détaillés de chaque élément.

Le **Gestionnaire de tâches** présente tous les processus, services et tâches qui sont exécutés sur votre appareil. ESET Endpoint Security permet d'arrêter les processus, services et tâches qui ne sont pas exécutés par le système. Ils sont indiqués par une icône rouge (**x**).

8. Administration à distance

ESET Remote Administrator (ERA) vous permet de gérer ESET Endpoint Security dans un environnement réseau, directement à partir d'un emplacement centralisé.

Les administrateurs peuvent effectuer les actions suivantes à distance :

- créer une tâche de configuration dans ERA et transmettre les paramètres à ESET Endpoint Security,
- déclencher une analyse à la demande,
- installer des mises à jour dans la base des signatures de virus,
- examiner les fichiers journaux,
- envoyer des messages d'administrateur aux appareils mobiles.

ERA permet d'améliorer votre niveau de sécurité et de faciliter l'administration de tous les produits ESET sur les stations de travail et les appareils mobiles clients. Les appareils mobiles avec ESET Endpoint Security peuvent se connecter à ERA à l'aide de tout type de connexion Internet (LAN, WLAN, réseau cellulaire 3G, HSDPA, GPRS, etc.) tant qu'il s'agit d'une connexion Internet normale (sans proxy, pare-feu, etc.) et si les deux extrémités sont correctement configurées. La réussite d'une connexion à ERA sur un réseau cellulaire dépend de l'opérateur GSM et nécessite une connexion Internet non limitée. Par exemple, si seule la navigation Web http est autorisée sur le port 8O, la connexion échouera, car le port 2222 est nécessaire pour la communication avec le serveur ERA.

Paramètres

Les options de paramétrage de l'administration à distance sont accessibles dans le menu principal de ESET Endpoint Security. Appuyez sur **Administration à distance** > **Paramètres**.

Activez l'administration à distance en sélectionnant l'option **Se connecter au serveur d'administration à distance**.

Intervalle entre les connexions au serveur - Cette option indique la fréquence à laquelle ESET Endpoint Security essaiera de se connecter au ERA Server pour envoyer les données.

Serveur principal, **Serveur secondaire** - Habituellement, seul le serveur principal a besoin d'être configuré. Si vous exécutez plusieurs serveurs ERA sur le réseau, vous pouvez opter pour l'ajout d'une connexion ERA Server secondaire. Elle sera utilisée comme solution de redémarrage après défaillance. Si le serveur principal devient inaccessible, ESET Endpoint Security contacte automatiquement le ERA Server secondaire. Il essaie simultanément de rétablir la connexion au serveur principal. Une fois que cette dernière est à nouveau active, ESET Endpoint Security retourne sur le serveur principal. La configuration de deux profils de serveur d'administration à distance est particulièrement recommandée pour les clients se connectant à la fois à partir du réseau local et depuis l'extérieur du réseau.

Adresse du serveur - Indique le nom DNS ou l'adresse IP du serveur exécutant ERA Server.

Port - Ce champ contient le port de serveur prédéfini utilisé pour la connexion. Nous vous recommandons de laisser le port par défaut défini sur 2222.

Si ESET Remote Administrator nécessite une authentification par mot de passe, sélectionnez l'option **Le serveur d'administration à distance nécessite une authentification** et entrez votre mot de passe dans le champ **Mot de passe**.

REMARQUE : pour plus d'informations sur la procédure de gestion du réseau à l'aide de ESET Remote Administrator, reportez-vous au manuel ESET Remote Administrator Installation Manual and User Guide (ce document n'est pas disponible dans votre langue).

9. Mise à jour

ESET Endpoint Security peut facilement être mis à jour à la dernier version du produit pour assurer la protection de votre appareil mobile contre les menaces et les attaques malveillantes les plus récentes. Si vous recevez une notification indiquant qu'une nouvelle de ESET Endpoint Security est disponible pour téléchargement, ESET vous recommande de l'installer dès que possible.

Par défaut, ESET Endpoint Security est installé avec une tâche qui garantit la mise à jour régulière du programme. Pour exécuter la mise à jour manuellement, appuyez sur **Mettre à jour maintenant** .

Paramètres

L'option **Mise à jour automatique** permet de définir l'intervalle de téléchargement automatique des mises à jour des signatures de virus.

REMARQUE : afin d'éviter toute utilisation superflue de la bande passante, les mises à jour sont publiées uniquement lorsque c'est nécessaire, c'est-à-dire lorsqu'une nouvelle menace est ajoutée. Les mises à jour sont gratuites avec votre licence active, mais votre opérateur de téléphonie mobile peut facturer le transfert des données.

10. Mot de passe

Votre mot de passe de sécurité protège les paramètres de toute modification non autorisée. Le mot de passe est nécessaire dans les cas suivants :

- Accès aux fonctionnalités protégées par mot de passe d'ESET Endpoint Security (Antivirus, Antispam, Anti-vol et Audit de sécurité)
- Accès à votre téléphone s'il a été verrouillé
- Envoi à votre appareil de commandes SMS
- Désinstallation d'ESET Endpoint Security

REMARQUE : la désinstallation de la protection est disponible uniquement sur Android 2.2 et les versions ultérieures.

Pour définir un nouveau mot de passe de sécurité, saisissez-le dans les champs **Mot de passe** et **Ressaisissez MdP**. L'option **Phrase de rappel** (si elle est définie) affiche une astuce qui vous permet de vous remémorer votre mot de passe si vous l'avez oublié.

IMPORTANT : choisissez votre mot de passe avec soin, car vous en aurez besoin pour déverrouiller votre appareil mobile ou désinstaller ESET Endpoint Security.

Dans l'onglet **Appliquer à**, vous pouvez indiquer les modules qui seront protégés par le mot de passe.

Si vous avez oublié votre mot de passe, vous pouvez envoyer à votre appareil mobile un SMS depuis le numéro d'un téléphone mobile enregistré dans la liste **Contacts administrateur**. Ce SMS doit avoir la forme suivante :
eset remote reset
Votre mot de passe sera réinitialisé.

11. Dépannage et assistance

11.1 Dépannage

ESET Endpoint Security offre une fonctionnalité de journalisation avancée qui contribue au diagnostic des problèmes techniques potentiels. Avant de contacter le service client d'ESET, il est fortement recommandé de rechercher une solution possible dans la base de connaissances ESET. Si vous devez néanmoins contacter le service client d'ESET, procédez comme suit :

1. Accédez au menu principal de ESET Endpoint Security, appuyez sur le bouton **MENU** et sélectionnez **Paramètres de journalisation**.
2. Sélectionnez un composant du programme auquel le problème est lié.
3. Répliquez le problème. Des informations seront consignées dans un fichier journal de l'application.
4. Accédez au menu principal de ESET Endpoint Security, appuyez sur le bouton **MENU** et sélectionnez **Service client**.
5. Si vous n'avez pas trouvé de solution dans notre base de connaissances, appuyez sur **Continuer**.
6. Remplissez tous les détails et appuyez sur **Soumettre** au bas de l'écran. Assurez-vous que l'option **Journal de l'application** est sélectionnée (par défaut).

11.2 Assistance technique

Les experts de notre service client sont disponibles pour vous apporter une assistance administrative ou technique concernant ESET Endpoint Security ou tout autre produit ESET.

Pour trouver des réponses aux questions les plus fréquentes, accédez à la base de connaissances ESET : *http://kb.eset.com/android*

La base de connaissances contient un grand nombre d'informations utiles qui permettent de résoudre les problèmes les plus courants. Elle est organisée en catégories et propose une fonction de recherche avancée.

Pour contacter le service client ESET, utilisez le formulaire de demande d'assistance disponible à cette adresse :
http://support.athena-gs.fr/demande_de_support.php?editeur=eset

Pour envoyer une demande d'assistance directement à partir de votre téléphone mobile, accédez au menu principal ESET Endpoint Security, puis appuyez sur le bouton **MENU** et sur **Service client**. Remplissez tous les champs obligatoires. Pour inclure **Journal de l'application** complet, suivez la procédure décrite dans la section Dépannage 12.